Brief Explanation of the Japanese Publication No. 4-216158

Date of Publication: August 6, 1992
Application No.: 3-36668
Date of Filing: February 7, 1991
Foreign Application Priority Data: February 15, 1990 – USA ... 480437
(USP 5,263,157)
Title of the Invention: Method and system for providing user access control within a distributed data processing system by the exchange of access control profiles
Inventor: Frederick L. Janis, Texas, U.S.A.
Applicant: International Business Machines Corporation (U.S.A.)

A method is disclosed for providing user access control for a plurality of resource objects within a distributed data processing system having a plurality of resource managers. A reference monitor service is established and a plurality of access control profiles are stored therein. Thereafter, selected access control profiles are exchanged between the reference monitor service and a resource manager in response to an attempted access of a particular resource object controlled by that resource manager. The resource manager may then control access to the resource object by utilizing the exchanged access control profile. In a preferred embodiment of the present invention, each access control profile may include access control information relating to a selected user; a selected resource object; a selected group of users; a selected set of resource objects; or, a predetermined set of resource objects and a selected group of users.

P-571

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平4－216158

(43)公開日　平成４年(1992)８月６日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/16	３８０　Ｄ	9190－5Ｌ		
13/00	３５７　Ｚ	7368－5Ｂ		

審査請求　有　　請求項の数12(全　８　頁)

(21)出願番号　特願平3－36668

(22)出願日　平成３年(1991)２月７日

(31)優先権主張番号　４８０４３７

(32)優先日　1990年２月15日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　フレデリック・エル・ジャニズ
アメリカ合衆国76278、テキサス州、ケラー、クウエイル・ラン　812番地

(74)代理人　弁理士　頓宮　孝一　（外４名）

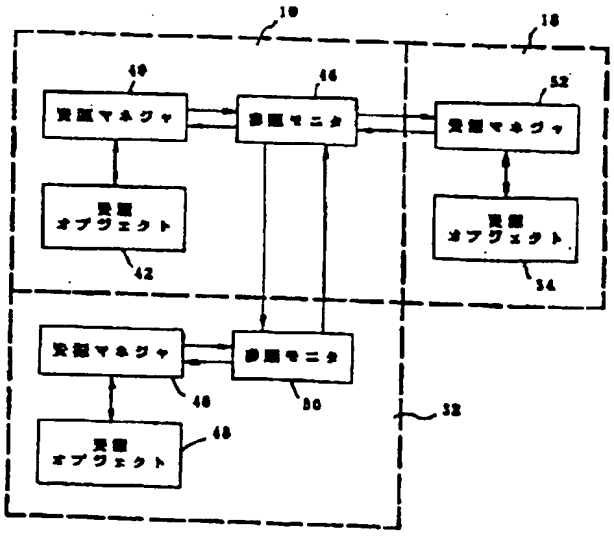
(54)【発明の名称】　分散データ処理システム内でユーザ・アクセスの制御を実現する方法

(57)【要約】

【目的】複数の資源マネジャを有する分散データ処理システム内で複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法を提供する。

【構成】参照モニタ・サービス（４４、５０）を確立し、複数のアクセス制御プロファイルをそこに記憶する。その後、ある資源マネジャ（４０、４６、５２）によって制御される特定の資源オブジェクト（４２、４８、５４）へのアクセスの試みに応答して、選択されたアクセス制御プロファイルが、参照モニタ・サービスとその資源マネジャの間で交換される。その後、資源マネジャは、交換されたアクセス制御プロファイルを用いて、その資源オブジェクトに対するアクセスを制御する。

【効果】分散データ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が実現される。



1

【特許請求の範囲】

【請求項1】複数の資源オブジェクトに関連づけられた複数の資源マネジャを有する分散データ処理システム内で前記複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法であって、参照モニタ・サービス内に、複数のアクセス制御プロファイルを記憶するステップと、特定の資源オブジェクトへのアクセスの試みに応答して、前記参照モニタ・サービスと選択された資源マネジャの間で、選択されたアクセス制御プロファイルを交換するステップと、前記資源マネジャを利用して、前記選択されたアクセス制御プロファイルに従って、前記特定の資源オブジェクトに対するアクセスを制御するステップとを含む、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項2】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項3】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された資源オブジェクトに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項4】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザ・グループに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項5】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された1組の資源オブジェクトに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項6】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ所定の1組の資源オブジェクトと、それぞれが前記所定の2組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストとに関するアクセス制御情報を含む、請求項1に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項7】複数の資源オブジェクトに関連づけられた複数の資源マネジャを有する分散データ処理システム内で前記複数の資源オブジェクトに対するユーザ・アクセスの制御を実現する方法であって、前記分散データ処理システム内で参照モニタ・サービスを確立するステップと、前記参照モニタ・サービス内に、複数のアクセス制御プロファイルを記憶するステップと、特定の資源オブジェクトへのアクセスの試みに応答して、前記参照モニタ・サービスと選択された資源マネジャの間で、選択されたアクセス制御プロファイルを交換するステップと、前記資源マネジャを利用して、前記選択されたアクセス制御プロファイルに従って、前記特定の資源オブジェクトに対するアクセスを制御するステップとを含む、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

2

【請求項8】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項9】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された資源オブジェクトに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項10】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択されたユーザ・グループに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項11】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ選択された1組の資源オブジェクトに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【請求項12】前記複数のアクセス制御プロファイルから選択されたプロファイルがそれぞれ所定の1組の資源オブジェクトと、それぞれが前記所定の1組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストとに関するアクセス制御情報を含む、請求項7に記載の、分散データ処理システム内でユーザ・アクセスの制御を実現する方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一般にデータ処理システムに関するものであり、具体的には、分散データ処理システム内の複数の資源オブジェクトに対するアクセスの制御を実現する、改良された方法に関するものである。さらに具体的にいうと、本発明は、分散データ処理システム全体を通じて、アクセス制御情報の高速かつ効率的な交換を可能にするシステムに関するものである。

【0002】

【従来の技術】コンピュータに基づくデータ処理システムにおける、セキュリティおよびアクセス制御システムは、当技術分野で公知である。既存のアクセス制御システムは、一般に、単一ホスト・システム本位のものである。前述の単一ホスト・アクセス制御システムは、ホストのセキュリティと、ファイルなどのシステム資源およびアプリケーションに対するアクセス制御とを実現する

3

ために利用される。それぞれのアプリケーションは、一般に、そのアプリケーションによって制御される資源に対するアクセス制御を実現しなければならない。

【0003】IBM370システムと共に使用するように設計されたアクセス制御システムの1例が、RACF（資源アクセス管理機能）と称する製品である。RACFは、ファイルやCICS（顧客情報管理システム）トランザクションなど、アプリケーションに対するアクセス制御を提供し、ユーザのアクセス権限レベルおよびグループ化に関して階層本位になっている。RACFは、「パスワード」本位のアクセス制御システムであり、ユーザ個人の識別と、その識別を検証するのに適したパスワードをユーザが知っているかどうかに基づいて、アクセスが許可または拒否される。しかし、RACFは、単一ホストシステム本位のものであり、別々の資源オブジェクトのグループに関連づけられた複数のホストを使用する、分散データ処理システムでは使用できない。というのは、このシステムでは、あるホストから別のホストへのアクセス制御情報の交換が可能でないからである。

【0004】既知のアクセス制御システムのもう1つの例が、AS／400である。AS／400システムは、ケイパビリティ（資格）に基づくシステムであり、セキュリティは、それぞれの資源オブジェクトに基づいている。各ユーザは、そのユーザのシステム内でのケイパビリティに基づいて、個々の資源オブジェクトにアクセスする権限を与えられる。AS／400システムは、ユーザ・プロファイル、オブジェクト権限およびシステム値をマシン自体のアーキテクチャ内で保持することによって、セキュリティを維持する。上記と同様に、このシステムは、単一のホストによって制御される資源オブジェクトへのアクセスを制御する点では非常に効率的であるが、複数のホストを含む分散データ処理システム内にある資源オブジェクトへのアクセスは制御できない。すなわち、あるホストによって制御されている資源オブジェクトへのアクセス権を、第2のホストに登録されたユーザが得ることはできない。

【0005】アクセス制御システムのもう1つの例が、製品DB2（データベース2）である。この製品は、より柔軟なアクセス制御が可能であり、細分的なまたはバンドルされたアクセス制御権限を提供する。たとえば、DB2システムは、システム管理用またはデータベース操作用の特別な権限を利用できる。さらに、アクセス特権を指定された権限または役割にまとめて、ユーザが、そのユーザ個人の識別ではなく、そのユーザの肩書または権限レベルに基づいて、特定の資源オブジェクトにアクセスできるようにすることができる。しかし、上記と同様に、DB2システムは、非DB2アプリケーションとアクセス制御情報を交換する能力をもたない。

【0006】

【発明が解決しようとする課題】したがって、分散データ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が必要であることは明白である。

4

【0007】したがって、本発明の1つの目的は、改良されたデータ処理システムを提供することである。

【0008】本発明の他の目的は、分散データ処理システム内の複数の資源オブジェクトに対するアクセス制御を実現する、改良された方法を提供することである。

【0009】本発明の他の目的は、分散データ処理システム内の複数の資源オブジェクトに対するアクセス制御を実現し、分散データ処理システム全体を通じて、高速かつ効率的なアクセス制御情報の交換を可能にする、改良された方法を提供することである。

【0010】

【課題を解決するための手段】前述の目的は、以下に述べるようにして達成される。本発明の方法を利用して、複数の資源マネジャを有する分散データ処理システム内で複数の資源オブジェクトに対するユーザ・アクセスの制御を実現することができる。参照モニタ・サービスを確立し、複数のアクセス制御プロファイルをそこに記憶する。その後、ある資源マネジャによって制御される特定の資源オブジェクトへのアクセスの試みに応答して、選択されたアクセス制御プロファイルが、参照モニタ・サービスとその資源マネジャの間で交換される。その後、資源マネジャは、交換されたアクセス制御プロファイルを用いて、その資源オブジェクトに対するアクセスを制御することができる。本発明の好ましい実施例では、それぞれのアクセス制御プロファイルは、選択されたユーザ、選択された資源オブジェクト、選択されたユーザ・グループ、選択された資源オブジェクト・グループ、あるいは所定の1組の資源オブジェクトと、それぞれが前記所定の1組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストに関するアクセス制御情報を含む。

【0011】

【実施例】図面、特に図1を参照すると、本発明の方法を実施するために利用される分散データ処理システム8が示されている。図からわかるように、分散データ処理システム8は、ローカル・エリア・ネットワーク（LAN）10と32など複数のネットワークを含み、それぞれのネットワークは、それぞれ複数の個々のコンピュータ12および30を含むことが好ましい。もちろん、前述のネットワークのそれぞれに、ホスト・プロセッサに結合された複数の対話型ワーク・ステーション（IWS）を使用してもよいことは、当業者には理解されよう。

【0012】このようなデータ処理システムでは一般的なことであるが、それぞれのコンピュータは、記憶装置

5

１４またはプリンタ／出力装置１６あるいはその両方に結合することができる。本発明の方法によれば、１つまたは複数の前述の記憶装置１４を利用して、分散データ処理システム８内の任意のユーザによって定期的にアクセスされるアプリケーションまたは資源オブジェクトを記憶することができる。記憶装置１４に記憶された前述のアプリケーションまたは資源オブジェクトはそれぞれ、当技術分野で周知の方式で資源マネジャに関連づけられる。資源マネジャは、それに関連づけられたすべての資源オブジェクトを維持し更新する責任を負う。

【００１３】図１によれば、分散データ処理システム８は、メイン・フレーム・コンピュータ１８など、複数のメイン・フレーム・コンピュータをも含む。これらのメイン・フレーム・コンピュータは、通信リンク２２によってＬＡＮ１０に結合することが好ましい。メイン・フレーム・コンピュータ１８は、ＬＡＮ１０用の遠隔記憶装置として働く記憶装置２０にも結合される。同様に、ＬＡＮ１０は、通信リンク２４を介し、サブシステム制御装置／通信制御装置２６および通信リンク３４を通じて、ゲートウェイ・サーバ２８に結合される。ゲートウェイ・サーバ２８は、ＬＡＮ３２をＬＡＮ１０にリンクする働きをする、独立のコンピュータまたはＩＷＳであることが好ましい。

【００１４】ＬＡＮ３２およびＬＡＮ１０に関して上述したように、資源オブジェクトは、記憶装置２０内に記憶され、記憶されたその資源オブジェクト用の資源マネジャとしてのメイン・フレーム・コンピュータ１８によって制御される。もちろん、メイン・フレーム・コンピュータ１８は、地理的にＬＡＮ１０から非常に遠く離れた所にあってよく、同様に、ＬＡＮ１０も、ＬＡＮ３２から離れた所にあってよいことが、当業者には理解されよう。すなわち、ＬＡＮ３２がカリフォルニアにあり、ＬＡＮ１０がテキサスにあり、メイン・フレーム・コンピュータ１８がニューヨークにあってもよい。

【００１５】この形式の既知の従来技術のシステムでは、個々のコンピュータ３０のユーザが、メイン・フレーム・コンピュータ１８に関連する記憶装置２０に記憶されたある資源オブジェクトにアクセスしたいと望む場合、コンピュータ３０のユーザが、メイン・フレーム・コンピュータ１８のセキュリティ・システムに登録される必要がある。これは、コンピュータ３０のユーザが、所望の資源オブジェクトへのアクセスを得るのに適当なパスワードを提示するために必要である。もちろん、この技法が、図１に示したデータ処理システムなどの分散データ処理システムではうまく働かないことは、当業者には理解されよう。

【００１６】次に図２を参照すると、本発明の方法と共に利用されるアクセス制御システムが、ブロック図で示されている。図によれば、ＬＡＮ１０および３２は破線で示されており、メイン・フレーム・コンピュータ１８

6

も同様である。いずれの場合も、資源オブジェクト４２、４８、５４が、図１の分散データ処理システム８のそれぞれの部分と関連づけて示されている。もちろん、図の各オブジェクトは、分散データ処理システム８のそれぞれの部分に関連する１つまたは複数の記憶装置に記憶される。図に示されるように、ＬＡＮ１０は、選択された資源オブジェクトを管理するために利用される１つまたは複数の個別のコンピュータである、資源マネジャ４０を含む。ＬＡＮ１０の内部には、参照モニタ４４も確立されている。参照モニタ４４は、本発明の方法によれば、アクセス制御プロファイルを記憶するのに利用されるアプリケーションまたはサービスであり、アクセス制御プロファイルは、選択されたユーザ、選択された資源オブジェクト、選択されたユーザ・グループ、選択された資源オブジェクト・グループ、あるいは所定の１組の資源オブジェクトと、それぞれが前記所定の１組の資源オブジェクトの少なくとも一部分へのアクセスを許可されているユーザの選択されたリストに関するアクセス制御情報を含む。

【００１７】さらに図２を参照すると、ＬＡＮ３３の内部に、当技術分野で周知の方式で資源オブジェクト４８へのアクセスを制御するために利用される、資源マネジャ４６が示されている。同様に、参照モニタ５０が、ＬＡＮ３２内に確立されている。前述したように、参照モニタ５０を利用して、ＬＡＮ３２内の個々のユーザならびにＬＡＮ３２内に記憶されている資源オブジェクトに関するアクセス制御プロファイルを記憶することが好ましい。

【００１８】最後に、メイン・フレーム・コンピュータ１８は、１つまたは複数の資源オブジェクト５４と関連づけられた、資源マネジャ５２を含むものとして図示されている。

【００１９】本発明の重要な特徴によれば、資源オブジェクト４２、４８、５４などの資源オブジェクトにアクセスを試みると、自動的に、１つまたは複数の参照モニタ・アプリケーションに対して、関連する資源マネジャが照会を行い、要求されたアクセスが許可されているか否かを判定する。本発明の図示の実施例によれば、データ処理システム８に必要な参照モニタ・アプリケーションは１つだけであるにもかかわらず、２つが図示されていることに留意されたい。本発明の方法によれば、各資源マネジャがすべて分散データ処理システム８内にある状態で、単一の参照モニタ・アプリケーション間の通信リンクが確立され（図１参照）、その結果、選択された資源オブジェクトへのアクセスを、その参照モニタ内のプロファイルに記憶されたアクセス制御情報に従って制御することができる。

【００２０】このようにして、ＬＡＮ３２内のユーザは、図１に示した通信リンク（２２、２４、３４）を介して、メイン・フレーム・コンピュータ１８に関連する

資源オブジェクト５４へのアクセスを要求できる。後でさらに詳しく説明するように、資源マネジャ５２は、次に、参照モニタ４４または参照モニタ５０あるいはその両方に照会を行って、要求されたアクセスを許可するプロファイルが存在するか否かを決定する。存在する場合は、そのプロファイル情報が、適当な参照モニタと資源マネジャ５２の間で交換され、資源オブジェクト５４へのアクセスが許可される。

【００２１】次に図３を参照すると、本発明の方法によるアクセス制御システムの確立を示す、高水準流れ図が示されている。図に示すように、ブロック６０で処理が始まり、その後ブロック６２に移って、あるオブジェクトまたはオブジェクト・グループ（４２、４８、５４）用のアクセス制御プロファイルが、関連する資源マネジャ（４０、４６、５２）によって定義される。その後、ブロック６４で、そのプロファイルが参照モニタ・アプリケーション（４４、５０）に記憶される。次に、ブロック６６で、アクセス制御プロファイルの確立を必要とするオブジェクトが他にもまだあるか否かを判定し、存在する場合には、ブロック６２に戻って、それ以降繰り返して続行する。

【００２２】アクセス制御プロファイルを必要とする資源オブジェクトが他にもうない場合は、ブロック６８に移って、関連する資源マネジャ（４０、４６、５２）が、分散データ処理システム８内の１人または複数のユーザに対するアクセス制御プロファイルを確立する。その後、ブロック７０で、このようにして作成されたアクセス制御プロファイルを、関連する参照モニタ・アプリケーション（４４、５０）に記憶する。次にブロック７２で、アクセス制御プロファイルの作成を必要とするユーザがデータ処理システム８内に他にまだいるか否かを判定する。まだいる場合は、上述と同様に、ブロック６８に戻って、追加のプロファイルを定義する。アクセス制御プロファイルを必要とするユーザが他にもういない場合は、ブロック７４で、処理は終了する。もちろん、このようにして、１つの資源オブジェクト、資源オブジェクト・グループ、１人のユーザ、ユーザ・グループ、あるいは所定の１組の資源オブジェクトと選択されたユーザ・グループに関するアクセス制御情報を含む様々なアクセス制御プロファイルを作成できることが、当業者には理解されよう。

【００２３】最後に、図４を参照すると、本発明の方法による資源オブジェクトへのアクセスを示す、高水準の流れ図が示されている。図に示すように、ブロック８０で処理が始まり、その後ブロック８２に移って、資源マネジャ（４０、４６、５２）が、その資源マネジャの範囲内にある資源オブジェクト（４２、４８、５４）に対するアクセス要求を受け取る。次に、ブロック８４に移って、最も近くにある参照モニタ・アプリケーション（４４、５０）の照会を行って、問題の資源オブジェクトまたはユーザに対するアクセス制御プロファイルが存在するか否かを判定する。

【００２４】次にブロック８６で、適当なアクセス制御プロファイルが局所で定義されているか否かを判定し、定義されている場合には、ブロック８８で、その特定の資源オブジェクトへのアクセスが許可されているか否かを判定する。この判定は、当業者には理解されるように、定義されたアクセス制御プロファイルを、問題の資源オブジェクトおよびユーザのパラメータと比較するだけのことである。その後、ブロック８８での判定で許可される場合、ブロック９０で、資源オブジェクトへのアクセスが提供され、その後ブロック９２で処理が終了する。

【００２５】ブロック８６に戻って、アクセス制御プロファイルが局所で定義されていない場合は、ブロック９４で、適当なアクセス制御プロファイルがシステム内のどこかで定義されているか否かを判定する。定義されている場合は、ブロック９６でそのプロファイルを検索し、次にブロック８８に戻って、選択された資源オブジェクトへのアクセスが許可されているか否かを判定する。その後、アクセスが許可される場合には、ブロック９０に移って、資源オブジェクトへのアクセスが行われ、その後処理が終了する。

【００２６】必要とされるアクセス制御プロファイルが、分散データ処理システム８（図１参照）内のどこでも定義されていないか、または所望の資源オブジェクトへのアクセスが許可されていないとブロック８８で判定された場合は、ブロック９８で、要求元へ適当なメッセージを送って、要求された資源オブジェクトへのアクセスを拒否する。

【００２７】以上の説明を参照すれば、それぞれが資源オブジェクトまたはユーザに関する１つまたは複数のアクセス制御プロファイルを含む、分散データ処理システム内の１つまたは複数の参照モニタ・アプリケーションを利用することによって、分散データ処理システム８内のそれぞれのユーザが、システム内のすべての地点にあるそれぞれの資源マネジャに登録する必要なしに、分散データ処理システムの様々な部分にある複数の資源オブジェクトへのアクセスを制御できることが、当業者には理解されよう。システム全体を通じたアクセス制御情報を含むアクセス制御プロファイルを、高速かつ効率的に交換できるようにすることによって、必要なアクセス制御の決定が限られた数の位置で行われ、処理の効率が大きく改善される。

【００２８】

【発明の効果】分散データ処理システムでのアクセス制御を実現し、これによって、システム全体を通じてのアクセス制御情報の交換によって、選択された資源オブジェクトへのアクセスを、分散データ処理システム全体を通じて制御する方法が実現された。

9

【図面の簡単な説明】

【図１】本発明の方法を実施するために利用できる分散データ処理システムを示す図である。

【図２】本発明の方法と共に利用されるアクセス制御システムのブロック図である。

【図３】本発明の方法によるアクセス制御システムの確立を示す、高水準の流れ図である。

【図４】本発明の方法による資源オブジェクトへのアクセスを示す、高水準の流れ図である。

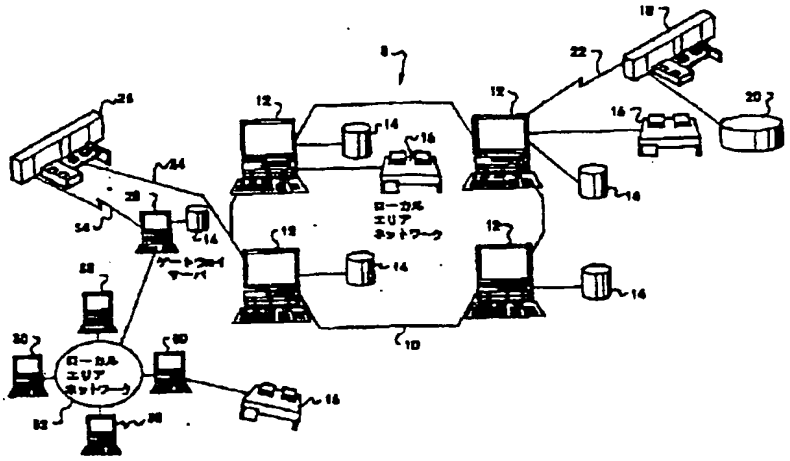
【符号の説明】

８　分散データ処理システム
１０　ローカル・エリア・ネットワーク（ＬＡＮ）
１２　コンピュータ
１４　記憶装置
１６　プリンタ／出力装置
１８　メイン・フレーム・コンピュータ

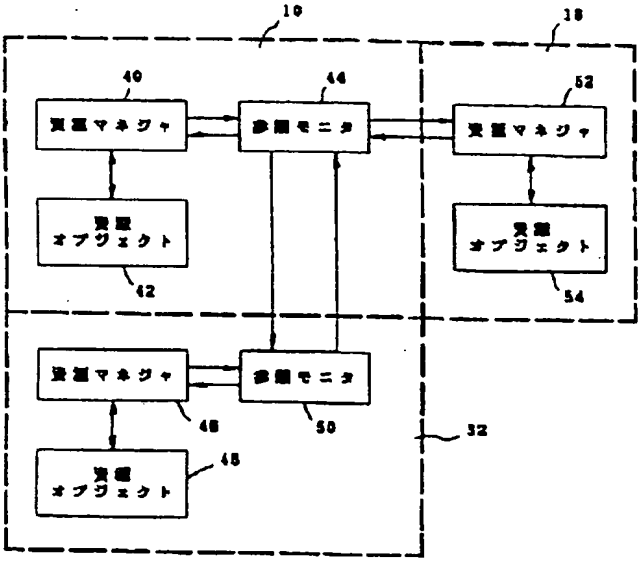
10

２０　記憶装置
２２　通信リンク
２４　通信リンク
２６　サブシステム制御装置／通信制御装置
２８　ゲートウェイ・サーバ
３０　コンピュータ
３２　ローカル・エリア・ネットワーク（ＬＡＮ）
３４　通信リンク
４０　資源マネジャ
４２　資源オブジェクト
４４　参照モニタ
４６　参照モニタ
４８　資源オブジェクト
５０　資源マネジャ
５２　資源オブジェクト
５４　参照モニタ

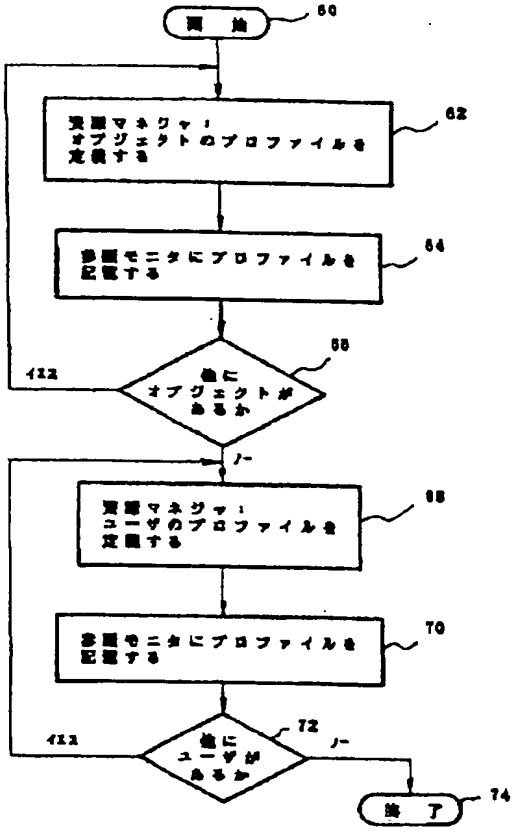
【図１】



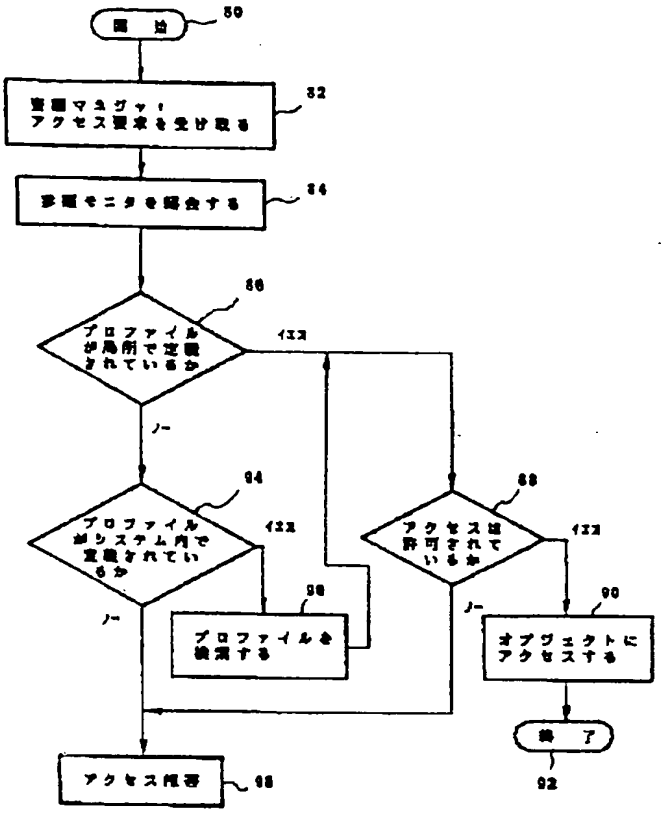
【図2】


10
18
40
44
52
資源マネジャ
参照モニタ
資源マネジャ
資源オブジェクト
資源オブジェクト
42
54
資源マネジャ
参照モニタ
46
50
32
資源オブジェクト
48

【図3】


開始
60
資源マネジャ：
オブジェクトのプロファイルを
定義する
62
参照モニタにプロファイルを
記憶する
64
他に
オブジェクトが
あるか
66
イエス
ノー
資源マネジャ：
ユーザのプロファイルを
定義する
68
参照モニタにプロファイルを
記憶する
70
他に
ユーザが
あるか
72
イエス
ノー
終了
74

【図4】


開　始
50
管理マネジャー
アクセス要求を受け取る
52
管理モニタを照会する
54
プロファイル
が局所で定義
されているか
56
YES
NO
プロファイル
がシステム内で
定義されてい
るか
94
YES
NO
プロファイルを
検索する
96
アクセスは
許可されて
いるか
98
YES
NO
オブジェクトに
アクセスする
90
終　了
92
アクセス拒否
58